CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-68
- After this Amendment: Claims 1-3, 7-22, 24-32, 36-51, 53-59 and 61-68

Non-Elected, Canceled, or Withdrawn claims: 4-6, 23, 33-35, 52 and 60

Amended claims: 1, 3, 7-9, 11, 19, 24-26, 30, 32, 36, 38, 40, 48, 53-55, 59, 61, 62, 65, 66 and 68

New claims: none

Claims:

1. **(Currently Amended)** A method comprising:

establishing authentication information, said authentication information including time information associated with authenticating logic;

with first logic, establishing credential information; ~~and~~

outputting an authentication request comprising said authentication information and said credential information, said authentication request being cryptographically modified;

with second logic that is operatively coupled to said first logic, modifying said authentication request by including certificate information in a modified authentication request;

with authenticating logic that is operatively configured to receive said modified authentication request, at least validating said authentication information, and authenticating said credential information; and

with said authenticating logic, outputting an authentication response comprising authentication approval information and corresponding cryptography information.

2. (Original) The method as recited in Claim 1, wherein said first logic is configured to output said authentication request.

3. (Currently Amended) The method as recited in Claim 1, wherein said second logic ~~this is operatively coupled to said first logic~~ is configured to output said modified authentication request.

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Currently Amended) The method as recited in Claim ~~6~~ 1, further comprising:

with said first logic, accessing at least a portion of said authentication response to retrieve said corresponding cryptography information and outputting said retrieved cryptography information.

8. (Currently Amended) The method as recited in Claim 7, further comprising:

with said second logic that is operatively coupled to said first logic and said authentication logic, accessing at least a portion of said authentication response and using said retrieved cryptography information retrieve said authentication approval information.

9. (Currently Amended) The method as recited in Claim ~~6~~ 1, further comprising:

with said second logic, accessing at least a portion of said authentication response to retrieve said corresponding cryptography information.

10. (Original) The method as recited in Claim 9, further comprising:

with said second logic, accessing at least a portion of said authentication response and using said retrieved cryptography information retrieve said authentication approval information.

11. (Currently Amended) The method as recited in Claim ~~6~~ 1, wherein said authentication request is cryptographically modified by encryption using a private key.

12. (Original) The method as recited in Claim 11, wherein said private key is associated with said first logic.

13. (Original) The method as recited in Claim 11, wherein said private key is associated with said second logic.

14. (Original) The method as recited in Claim 11, further comprising:

with said authenticating logic, retrieving said authentication information and said credential information from said authentication request using a public key pair-wise associated with said private key.

15. (Original) The method as recited in Claim 14, further comprising:

with said authenticating logic:

establishing a temporary key;

encrypting said temporary key using said public key to form said corresponding cryptography information; and

encrypting said authentication approval information using said temporary key.

16. (Original) The method as recited in Claim 15, further comprising:

with said second logic, providing said encrypted temporary key to said first logic; and

with said first logic, retrieving said temporary key from said encrypted temporary key using said private key.

17. (Original) The method as recited in Claim 16, further comprising:

with said first logic, providing said retrieved temporary key to said second logic; and

with said second logic, retrieving said authentication approval information using said retrieved temporary key.

18. (Original) The method as recited in Claim 15, wherein said temporary key includes a symmetric key.

19. (Currently Amended) The method as recited in Claim 8, wherein said first logic is ~~substantially~~ provided in at least a first device that includes a credential gathering mechanism configurable to establish said credential information, said second logic is provided in at least ~~partially in~~ a second device, and said authenticating logic is provided in at least ~~partially in~~ a third device.

20. (Original) The method as recited in Claim 19, wherein said credential gathering mechanism is configurable to establish biometric information.

21. (Original) The method as recited in Claim 19, wherein said second device includes at least one computer operatively configured as a client device, and said third device includes a computer operatively configured as a server device.

22. (Original) The method as recited in Claim 19, further comprising:

generating said authentication information using at least one logic selected from said second logic and said authenticating logic.

23. (Canceled)

24. (Currently Amended) The method as recited in Claim ~~23~~ 19, wherein said authenticating logic is configured to validate said authentication request based at least in part on said certificate information.

25. (Currently Amended) The method as recited in Claim ~~5~~ 1, wherein said authenticating logic is configured to validate said authentication information based on at least nonce data and timestamp data within said authentication information.

26. (Currently Amended) The method as recited in Claim ~~5~~ 1, wherein said authenticating logic is configured to authenticate said credential

information by logically comparing said credential information with stored credential information.

27. (Original) The method as recited in Claim 8, wherein said authentication approval information includes an access token for use by said second device.

28. (Original) The method as recited in Claim 1, wherein said authentication information includes nonce data and said time information includes timestamp data.

29. (Original) The method as recited in Claim 1, wherein said authentication request includes at least one type of data selected from a group of data comprising identifier data, nonce data, signature data, timestamp data, and credential data.

30. (Currently Amended) A computer readable medium having computer implementable instructions for causing one or more processing units to perform acts comprising:

establishing authentication information, said authentication information including time information associated with authenticating logic;

outputting an authentication request comprising said authentication information and credential information, said authentication request being cryptographically modified;

with second logic that is operatively coupled to said first logic, modifying said authentication request by including certificate information in a modified authentication request;

with authenticating logic that is operatively configured to receive said modified authentication request, at least validating said authentication information, and authenticating said credential information; and

with said authenticating logic, outputting an authentication response comprising authentication approval information and corresponding cryptography information.

31. (Original) The computer readable medium as recited in Claim 30, wherein first logic is configured to output said authentication request.

32. (Currently Amended) The computer readable medium as recited in Claim 31, wherein said second logic ~~this is operatively coupled to said first logic~~ is configured to output said authentication request and said first logic is configured to provide said credential information.

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Currently Amended) The computer readable medium as recited in Claim ~~35~~ 30, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said first logic, accessing at least a portion of said authentication response to retrieve said corresponding cryptography information and outputting said retrieved cryptography information.

37. (Original) The computer readable medium as recited in Claim 36, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with second logic that is operatively coupled to said first logic and said authentication logic, accessing at least a portion of said authentication response and using said retrieved cryptography information retrieve said authentication approval information.

38. (Currently Amended) The computer readable medium as recited in Claim ~~35~~ 30, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said second logic, accessing at least a portion of said authentication response to retrieve said corresponding cryptography information.

39. (Original) The computer readable medium as recited in Claim 38, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said second logic, accessing at least a portion of said authentication response and using said retrieved cryptography information retrieve said authentication approval information.

40. (Currently Amended) The computer readable medium as recited in Claim ~~35~~ 30, wherein said authentication request is cryptographically modified by encryption using a private key.

41. (Original) The computer readable medium as recited in Claim 40, wherein said private key is associated with said first logic.

42. (Original) The computer readable medium as recited in Claim 40, wherein said private key is associated with said second logic.

43. (Original) The computer readable medium as recited in Claim 40, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said authenticating logic, retrieving said authentication information and said credential information from said authentication request using a public key pair-wise associated with said private key.

44. (Original) The computer readable medium as recited in Claim 43, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said authenticating logic:

establishing a temporary key;

encrypting said temporary key using said public key to form said corresponding cryptography information; and

encrypting said authentication approval information using said temporary key.

45. (Original) The computer readable medium as recited in Claim 44, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said second logic, providing said encrypted temporary key to said first logic; and

with said first logic, retrieving said temporary key from said encrypted temporary key using said private key.

46. (Original) The computer readable medium as recited in Claim 45, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

with said first logic, providing said retrieved temporary key to said second logic; and

with said second logic, retrieving said authentication approval information using said retrieved temporary key.

47. (Original) The computer readable medium as recited in Claim 44, wherein said temporary key includes a symmetric key.

48. (Currently Amended) The computer readable medium as recited in Claim 37, wherein said first logic is ~~substantially~~ provided in at least a first device that includes a credential gathering mechanism configurable to establish said credential information, said second logic is provided in at least ~~partially in~~ a second device, and said authenticating logic is provided in at least ~~partially in~~ a third device.

49. (Original) The computer readable medium as recited in Claim 48, wherein said credential gathering mechanism is configurable to establish biometric information.

50. (Original) The computer readable medium as recited in Claim 48, wherein said second device includes at least one computer operatively configured as a client device, and said third device includes a computer operatively configured as a server device.

51. (Original) The computer readable medium as recited in Claim 48, having computer implementable instructions for causing one or more processing units to perform further acts comprising at least one of the following acts:

generating said authentication information using at least one logic selected from said second logic and said authenticating logic.

52. (Canceled)

53. (Currently Amended) The computer readable medium as recited in Claim ~~52~~ 48, wherein said authenticating logic is configured to validate said authentication request based at least in part on said certificate information.

54. (Currently Amended) The computer readable medium as recited in Claim ~~34~~ 30, wherein said authenticating logic is configured to validate said authentication information based on at least nonce data and timestamp data within said authentication information.

55. (Currently Amended) The computer readable medium as recited in Claim ~~34~~ 30, wherein said authenticating logic is configured to authenticate said credential information by logically comparing said credential information with stored credential information.

56. (Original) The computer readable medium as recited in Claim 37, wherein said authentication approval information includes an access token for use by said second device.

57. (Original) The computer readable medium as recited in Claim 30, wherein said authentication information includes nonce data and said time information includes timestamp data.

58. (Original) The computer readable medium as recited in Claim 30, wherein said authentication request includes at least one type of data selected from a group of data comprising identifier data, nonce data, signature data, timestamp data, and credential data.

59. (Currently Amended) A system comprising:

an authentication device having authentication logic;

a first device having first logic;

a second device having second logic that is operatively coupled to said authentication logic and said first logic; and

wherein:

at least one of said authenticating logic and said second logic is configured to provide authentication information to said first logic, said authentication information including time information associated with said authenticating logic;

said first logic is configured to establish credential information,

at least one logic selected from said first logic and second logic is configured to output an authentication request comprising said authentication information and said credential information, said authentication request being cryptographically modified;

said second logic is configured to output said authentication request; ~~and~~

said authenticating logic is configured to receive said authentication request, and at least validate said authentication information, and authenticate said credential information; and

said authenticating logic is further configured to output an authentication response comprising authentication approval information and corresponding cryptography information.

60. (Canceled)

61. (Currently Amended) The system as recited in Claim ~~60~~ 59, wherein said authentication approval information includes an access token for use by said second device.

62. (Currently Amended) The system as recited in Claim ~~60~~ 59, wherein:

said first logic is further configured to access at least a portion of said authentication response to retrieve said corresponding cryptography information and output said retrieved cryptography information; and

said second logic is further configured to access at least a portion of said authentication response and use said retrieved cryptography information output by said first logic to retrieve said authentication approval information.

63. (Original) The system as recited in Claim 62, wherein:

said first logic is further configured to cryptographically modify said authentication request by encryption using a private key; and

said authenticating logic is further configured to retrieve said authentication information and said credential information from said authentication request using a public key pair-wise associated with said private key.

64. (Original) The system as recited in Claim 63, wherein:

said authenticating logic is further configured to establish a temporary key, encrypt said temporary key using said public key to form said corresponding cryptography information, and encrypt said authentication approval information using said temporary key;

said second logic is further configured to provide said encrypted temporary key to said first logic;

said first logic is further configured to retrieve said temporary key from said encrypted temporary key using said private key, and provide said retrieved temporary key to said second logic; and

said second logic is further configured to retrieve said authentication approval information using said retrieved temporary key.

65. (Currently Amended) The system as recited in Claim ~~60~~ 59, wherein:

said second logic is further configured to access at least a portion of said authentication response to retrieve said corresponding cryptography information and use said retrieved cryptography information to retrieve said authentication approval information.

66. (Currently Amended) An apparatus comprising:

a credential gathering mechanism configurable to establish credential information;

first logic operatively coupled to said credential gathering mechanism and configured to access authentication information, said authentication information including time information associated with externally operating authenticating logic, and output an authentication request comprising said authentication information and said credential information, said authentication request being cryptographically modified;

second logic that is operatively coupled to said first logic, wherein said second logic modifies said authentication request by including certificate information in a modified authentication request.

wherein, said authenticating logic is configured to receive said modified authentication request, and at least validate said authentication information, and authenticate said credential information; and

said authenticating logic is further configured to output an authentication response comprising authentication approval information and corresponding cryptography information.

67. (Original) The apparatus as recited in Claim 66, wherein said credential information includes biometric credential information.

68. (Currently Amended) An apparatus comprising:

means for identifying authentication information that includes time information associated with authenticating logic;

means for establishing credential information;

means for outputting an authentication request comprising said authentication information and said credential information, said authentication request being cryptographically modified;

means for receiving said authentication request;

means for validating said authentication request;

means for validating said authentication information; ~~and~~

means for authenticating said credential information; and

means for outputting an authentication response comprising authentication approval information and corresponding cryptography information.